



TITLE:

Triply even codes について (デザイン、符号、グラフおよびその周辺)

AUTHOR(S):

別宮, 耕一

CITATION:

別宮, 耕一. Triply even codes について (デザイン、符号、グラフおよびその周辺). 数理解析研究所講究録 2013, 1844: 139-145

ISSUE DATE:

2013-07

URL:

<http://hdl.handle.net/2433/195021>

RIGHT:

Tripily even codes について

弘前大学・理工学研究科 別宮 耕一 (Koichi BETSUMIYA)
Graduate School of Science and Technology, Hirosaki University

概 要

まず, triply even code の極大性の判定法について述べる. 次に 2 種類の極大な triply even code の構成法を与える.

1 準備

本稿では, これまで知られているの極大な triply even codes が 2 つの無限系列からなることを述べる. なお, 本稿の内容は東北大学・宗政氏との共同研究 [2] の一部である.

最初に, よく知られた概念である doubly even code の類似として triply even code を定義する. まず, 用語の定義をする.

$\mathbb{F}_2 = \{0, 1\}$ を二元体とする. \mathbb{F}_2^n の k 次元部分空間 C を $[n, k]$ code と呼ぶ. また, $x = (x_1, x_2, \dots, x_n) \in C$ に対して, $\text{wt}(x) := |\text{supp}(x)| := |\{i \in \{1, 2, \dots, n\} \mid x_i \neq 0\}|$ を Hamming weight と呼ぶ. $x := (x_1, x_2, \dots, x_n), y := (y_1, y_2, \dots, y_n) \in \mathbb{F}_2^n$ に対して, 内積を $x \cdot y = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$ とする. C と C' が置換同値であるとは, code C の成分の順序を入れ替えることで C' が得られることをいい, $C \cong C'$ と表記する.

次の概念については多くの研究がなされている.

- 定義 1. (i) $[n, k]$ code $C \subset \mathbb{F}_2^n$ が doubly even code であるとは, 任意の $x \in C$ に対して, $\text{wt}(x) \equiv 0 \pmod{4}$ となることをいう.
- (ii) Doubly even code C が極大であるとは, $C' \supsetneq C$ となる doubly even code C' が存在しないこととする.
- (iii) $[n, k]$ code $C \subset \mathbb{F}_2^n$ が self dual code であるとは, $C = C^\perp := \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \ (\forall y \in C)\}$ を満たすことをいう.

doubly even code の類似として triply even code を次のように定義する.

- 定義 2. (i) $[n, k]$ code $C \subset \mathbb{F}_2^n$ が triply even code であるとは, 任意の $x \in C$ に対して, $\text{wt}(x) \equiv 0 \pmod{8}$ となることと定義する.
- (ii) Triply even code C が極大であるとは, $C' \supsetneq C$ となる triply even code C' が存在しないこととする.

2 極大性の判定法

本節では, triply even code に関する極大性の判定法について述べる.

まず, doubly even code について, 次はよく知られている事実であり, 容易に検証することができる.

命題 3. $n \equiv 0 \pmod{8}$ の場合, 次は同値である.

- (i) $C \subset \mathbb{F}_2^n$ が極大 doubly even code である.
- (ii) $C \subset \mathbb{F}_2^n$ が doubly even self dual code である.
- (iii) $C \subset \mathbb{F}_2^n$ が doubly even code で, $\dim C = \frac{n}{2}$ となる.

命題 3 は doubly even code の極大性が簡単に特徴付けできることを示している. しかし, 類似の概念である triply even code の極大性については, 事情が少々複雑となっている. ここではその判定法について述べる.

まず, 記号を準備する. ここで $C \subset \mathbb{F}_2^{n_1}$, $D \subset \mathbb{F}_2^{n_2}$ を codes とし, これらの直和を次のように定義する.

$$C \oplus D := \{(x_1, \dots, x_{n_1}, y_1, \dots, y_{n_2}) \in \mathbb{F}_2^{n_1+n_2} \mid (x_1, \dots, x_{n_1}) \in C, (y_1, \dots, y_{n_2}) \in D\}$$

言い換えると, M を (k_1, n_1) 行列, N を (k_2, n_2) 行列とし,

$$\begin{aligned} C &= \{(a_1, \dots, a_{k_1})M \mid (a_1, \dots, a_{k_1}) \in \mathbb{F}_2^{k_1}\}, \\ D &= \{(b_1, \dots, b_{k_2})N \mid (b_1, \dots, b_{k_2}) \in \mathbb{F}_2^{k_2}\} \end{aligned}$$

となるとき, これらの直和は次のように表すことができる.

$$C \oplus D = \left\{ (c_1, \dots, c_{k_1+k_2}) \left(\begin{array}{c|c} M & 0 \\ \hline 0 & N \end{array} \right) \mid (c_1, \dots, c_{k_1+k_2}) \in \mathbb{F}_2^{k_1+k_2} \right\}$$

code が自明でな 2 つの codes の直和と置換同値であるとき, 可約といい, そうでないとき既約であるという.

$C, D \subset \mathbb{F}_2^n$ を codes とする. $(x_1, \dots, x_n) * (y_1, \dots, y_n) := (x_1 y_1, \dots, x_n y_n)$ とし, 次のように記号を定義する.

$$\begin{aligned} C * D &:= \langle x * y \mid x \in C, y \in D \rangle \\ \text{rad } C &:= \{x \in C^\perp \mid \forall y \in C, \text{wt}(x * y) \equiv 0 \pmod{4}\} \\ \text{Rad } C &:= \{x \in \text{rad } C \mid \text{wt}(x) \equiv 0 \pmod{8}\} \end{aligned}$$

このとき, 次のような包含関係が成立する.

補題 4. $C \subset \mathbb{F}_2^n$ を code とすると,

$$\text{Rad } C \subset \text{rad } C \subset (C * C)^\perp \subset C^\perp$$

証明. $C = \{x * x \mid x \in C\}$ より, $C \subset C * C$ となり, $(C * C)^\perp \subset C^\perp$ である. 次に, $\text{rad } C \subset (C * C)^\perp$ を示す. $x \in \text{rad } C$, $y, z \in C$ とすると, $\text{wt}(x * (y + z)) = \text{wt}(x * y) + \text{wt}(x * z) - 2\text{wt}(x * y * z)$ となるので, $\text{wt}(x * y * z) \equiv 0 \pmod{2}$ となる. よって, $x \in (C * C)^\perp$ となる. \square

doubly even code の極大性に関して次が成立する.

補題 5. $C = \bigoplus_{i=1}^m C_i \subset \mathbb{F}_2^n$ を doubly even self dual code とし, 各 $C_i \subset \mathbb{F}_2^{n_i}$ を既約因子とする. 次が成立する.

$$\bigoplus_{i=1}^m \langle \mathbf{1}_{n_i} \rangle = \text{Rad } C = \text{rad } C = (C * C)^\perp$$

ただし, $\mathbf{1}_{n_i} = (1, \dots, 1) \in \mathbb{F}_2^{n_i}$ とする.

証明. まず, C を code とすると

$$\begin{aligned} x \in (C * C)^\perp &\iff \forall y, z \in C, \text{wt}(x * y * z) \equiv 0 \pmod{2} \\ &\iff \forall y \in C, x * y \in C^\perp \end{aligned}$$

となるので, $(C * C)^\perp * C \subset C^\perp$ となる. 従って, C が doubly even code であるとき, 次の包含関係が成立する.

$$C = \bigoplus_{i=1}^m \langle \mathbf{1}_{n_i} \rangle * C \subset (\text{rad } C) * C \subset (C * C)^\perp * C \subset C^\perp$$

ここで $C = C^\perp$ ならば, $\bigoplus_{i=1}^m \langle \mathbf{1}_{n_i} \rangle = \text{Rad } C = (C * C)^\perp$ となる. \square

Triply even code について, 次の包含関係が成立する.

補題 6. $n \equiv 0 \pmod{16}$, $C \subset \mathbb{F}_2^n$ を triply even code とすると, 次が成立する.

$$C \subset \text{Rad } C$$

証明. C を triply even code とし, $x, y \in C$ とすると, $\text{wt}(x) \equiv 0 \pmod{8}$ であり, $\text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2\text{wt}(x * y)$ となるので, $\text{wt}(x * y) \equiv 0 \pmod{4}$ となる. 従って, $C \subset \text{Rad } C$ となる. \square

Triply even code の極大性について, 次が成立する.

補題 7. $n \equiv 0 \pmod{16}$, $C \subset \mathbb{F}_2^n$ を triply even code とすると, 以下は同値である.

(i) C は極大 triply even code である.

(ii) $C = \text{Rad } C$.

証明. $x \in \mathbb{F}_2^n$ とし, C を triply even code とする. $\langle C, x \rangle$ が triply even code であることの必要十分条件は $x \in \text{Rad } C \cap (C * C)^\perp$ である. また, $\text{Rad } C \cap (C * C)^\perp = \text{Rad } C$ となるので, C が極大 triply even であることの必要十分条件は $C \supset \text{Rad } C$ である. つまり, $C = \text{Rad } C$ となることとなる. \square

3 Triply even code の構成法

ここから 2 種類の triply even code の構成法について述べる.

3.1 構成法 1 : doubly even self dual code を用いた方法

ここでは doubly even self dual code を用いた triply even code の構成法について述べる.

$C \subset \mathbb{F}_2^n$ を doubly even self dual code とする. このとき, R を $\text{Rad } C$ の生成行列とする. つまり, $m := \dim(\text{Rad } C)$ とし, (m, n) 行列 R を次を満たすものとする.

$$\text{Rad } C = \{(x_1, \dots, x_m) \cdot R \mid (x_1, \dots, x_m) \in \mathbb{F}_2^m\}$$

M を C の生成行列とする. つまり, (k, n) 行列 M を次を満たすものとする.

$$C = \{(x_1, \dots, x_k) \cdot M \mid (x_1, \dots, x_k) \in \mathbb{F}_2^k\}$$

このとき, 次のように $\tilde{\mathcal{D}}(C) \subset \mathbb{F}_2^{m+k}$ を定める.

$$\tilde{\mathcal{D}}(C) := \left\{ (x_1, \dots, x_{m+k}) \cdot \left(\begin{array}{c|c} 0 & R \\ \hline M & M \end{array} \right) \mid (x_1, \dots, x_{m+k}) \in \mathbb{F}_2^{m+k} \right\}$$

定理 8. doubly even self dual code C に対して, $\tilde{\mathcal{D}}(C)$ は極大 triply even code である.

証明. $C = \bigoplus_{i=1}^m C_i$ を C の既約分解とすると,

$$\begin{aligned} \tilde{\mathcal{D}}(C) &\cong \bigoplus_{i=1}^m \tilde{\mathcal{D}}(C_i) \\ \tilde{\mathcal{D}}(C) * \tilde{\mathcal{D}}(C) &\cong \bigoplus_{i=1}^m \tilde{\mathcal{D}}(C_i) * \tilde{\mathcal{D}}(C_i) \end{aligned}$$

$$C_i = \{(x_1, \dots, x_{k_i}) \cdot M_i \mid (x_1, \dots, x_{k_i}) \in \mathbb{F}_2^{k_i}\} \subset \mathbb{F}_2^{n_i}$$

とすると, 補題 5 より,

$$\langle 1_{n_i} \rangle^\perp = C_i * C_i = \{(x_1, \dots, x_{n_i-1}) \cdot M'_i \mid (x_1, \dots, x_{n_i-1}) \in \mathbb{F}_2^{n_i-1}\} \subset \mathbb{F}_2^{n_i}$$

と表すことができ, 次のように記述することができる.

$$\begin{aligned} \tilde{\mathcal{D}}(C_i) &= \left\{ (x_1, \dots, x_{k_i+1}) \cdot \left(\begin{array}{c|c} 0 & 1_{n_i} \\ \hline M_i & M_i \end{array} \right) \mid (x_1, \dots, x_{k_i+1}) \in \mathbb{F}_2^{k_i+1} \right\} \\ \tilde{\mathcal{D}}(C_i) * \tilde{\mathcal{D}}(C_i) &= \left\{ (x_1, \dots, x_{k_i+n_i-1}) \cdot \left(\begin{array}{c|c} 0 & M_i \\ \hline M'_i & M'_i \end{array} \right) \mid (x_1, \dots, x_{k_i+n_i-1}) \in \mathbb{F}_2^{k_i+n_i-1} \right\} \end{aligned}$$

また,

$$\left(\begin{array}{c|c} 0 & \mathbf{1}_{n_i} \\ \hline M_i & M_i \end{array} \right) \left(\begin{array}{c|c} 0 & M_i \\ \hline M'_i & M'_i \end{array} \right)^T = 0$$

となることより,

$$\tilde{\mathcal{D}}(C_i) \subset (\tilde{\mathcal{D}}(C_i) * \tilde{\mathcal{D}}(C_i))^\perp$$

加えて,

$$\dim \tilde{\mathcal{D}}(C_i) * \tilde{\mathcal{D}}(C_i) = 3n_i - 1$$

より,

$$\dim(\tilde{\mathcal{D}}(C_i) * \tilde{\mathcal{D}}(C_i))^\perp = n_i + 1 = \dim \tilde{\mathcal{D}}(C_i)$$

従って,

$$\tilde{\mathcal{D}}(C_i) = (\tilde{\mathcal{D}}(C_i) * \tilde{\mathcal{D}}(C_i))^\perp$$

従って, 補題 4, 補題 7 より, $\tilde{\mathcal{D}}(C_i)$ は極大な triply even code である. □

この事実により, doubly even self dual code C から極大な triply even code $\tilde{\mathcal{D}}(C)$ を構成することができることが分かる. 加えて, C が m 個の既約成分に分解されるとき, つまり, $C \cong \bigoplus_{i=1}^m C_i$ を C の既約分解とすると, $\dim \tilde{\mathcal{D}}(C) = m + \dim C$ が得られる. このことから, 長さが同じでも極大な triply even code の次元は一定ではないことが分かる.

3.2 構成法 2 : triangular graph を用いた方法

ここでは, triangular graph を用いた triply even code の構成法について述べる. まず, triangular graph の定義を述べる.

定義 9. n を正整数とし, $\Omega := \{1, 2, \dots, n\}$ とする. graph T_n の頂点 $V(T_n)$ と辺 $E(T_n)$ を次のように与えることで T_n を定義し, *triangular graph* と呼ぶ.

$$V(T_n) := \binom{\Omega}{2} = \{\alpha \subset \Omega \mid |\alpha| = 2\}$$

$$E(T_n) := \left\{ (\alpha, \beta) \in \binom{\Omega}{2} \times \binom{\Omega}{2} \mid |\alpha \cap \beta| = 1 \right\}$$

今, A を graph T_n の隣接行列とする. つまり, $V(T_n) = \{\alpha_1, \dots, \alpha_t\}$ ($t = \binom{n}{2}$) と表すとき, 各成分を次のように与える.

$$A_{ij} = \begin{cases} 0 & \text{if } |\alpha_i \cap \alpha_j| \neq 1 \\ 1 & \text{if } |\alpha_i \cap \alpha_j| = 1 \end{cases}$$

このとき、次のように $C(T_n) \subset \mathbb{F}_2^t$ を定める.

$$C(T_n) := \{(x_1, \dots, x_t) \cdot A \mid (x_1, \dots, x_t) \in \mathbb{F}_2^t\}$$

A の各行の weight は $2(n-2)$ となることは容易に確かめられる. 加えて, 次の性質は triangular graph について古くから知られていることからただちに導出される..

補題 10. $n \equiv 2 \pmod{4}$ のとき, $C(T_n)$ は次元 $n-2$ の triply even code になる.

さらに, 次の補題が成立する.

補題 11. $n \equiv 2 \pmod{4}$ のとき,

$$\dim(C(T_n) * C(T_n)) = \frac{(n-1)(n-2)}{2}$$

証明. $v_i \in \mathbb{F}_2^t$ を $\text{supp}(v_j) = \{i \in \{1, \dots, t\} \mid j \in \alpha_i\}$ となるようにとると, $\{v_1 + v_n, v_2 + v_n, \dots, v_{n-2} + v_n\}$ は $C(T_n)$ の基底になる. さらに, この基底から $\{v_1 + v_n, v_2 + v_n, \dots, v_{n-2} + v_n\} \cap \{(v_i + v_n) * (v_j + v_n) \mid 1 \leq i < j \leq n-2\}$ が $C(T_n) * C(T_n)$ の基底になることを示すことができる. 従って, $\dim(C(T_n) * C(T_n)) = \frac{(n-1)(n-2)}{2}$ が言える. \square

$C(T_n)$ の極大性について, 次の補題が成立する.

補題 12. $n \equiv 2 \pmod{4}$ のとき, $(C(T_n) * C(T_n))^\perp = C(T_n) + \langle \mathbf{1}_t \rangle$ となる. 特に $C(T_n)$ は極大な triply even code となる.

証明. $x, y, z \in C(T_n)$ に対して, $\text{wt}(x * y * z) \equiv 0 \pmod{2}$ より, $(C(T_n) * C(T_n))^\perp \supset C(T_n) + \langle \mathbf{1}_t \rangle$ となる. この両辺の次元を比較すると, 次の等号が成立する.

$$(C(T_n) * C(T_n))^\perp = C(T_n) + \langle \mathbf{1}_t \rangle$$

また, $t = \frac{n(n-1)}{2} \equiv 1 \pmod{2}$ となるので,

$$\text{Rad } C(T_n) = (C(T_n) * C(T_n))^\perp \cap \text{Rad } C(T_n) = C(T_n)$$

となる. 従って, 補題 7 より, $C(T_n)$ は極大な triply even code となる. \square

今, $C(T_n)$ の生成行列を B とする. つまり, B を次を満たすような $(n-2, t)$ 行列とする.

$$C(T_n) := \{(x_1, \dots, x_{n-2}) \cdot B \mid (x_1, \dots, x_{n-2}) \in \mathbb{F}_2^{n-2}\}$$

ここで, $l := 8\lceil \frac{t}{8} \rceil$, $l' := l - t$ とし, $\hat{C}(T_n)$ を次のように定義する.

$$\begin{aligned} \hat{C}(T_n) &:= \langle \mathbf{1}_l \rangle + C(T_n) \oplus \mathbf{0}_{l'} \\ &= \left\{ (x_1, \dots, x_{n-1}) \cdot \left(\frac{\mathbf{1}_t \mid \mathbf{1}_{l'}}{B \mid 0} \right) \mid (x_1, \dots, x_{n-1}) \in \mathbb{F}_2^{n-1} \right\} \end{aligned}$$

定理 13. $n \equiv 2 \pmod{4}$ のとき, $\hat{C}(T_n)$ は極大な triply even code となる.

証明. 次のように $(\hat{C}(T_n) * \hat{C}(T_n))^\perp$ を求めることができる.

$$\begin{aligned}
 (\hat{C}(T_n) * \hat{C}(T_n))^\perp &= (\langle \mathbf{1}_l \rangle + (C(T_n) * C(T_n)) \oplus \mathbf{0})^\perp \\
 &= \langle \mathbf{1}_l \rangle^\perp \cap ((C(T_n) * C(T_n))^\perp \oplus \mathbb{F}_2^{l'}) \\
 &= \langle \mathbf{1}_l \rangle^\perp \cap ((C(T_n) + \langle \mathbf{1} \rangle) \oplus \mathbb{F}_2^{l'}) \quad (\text{補題 12 より}) \\
 &= C(T_n) \oplus \langle \mathbf{1}_{l'} \rangle^\perp + \langle \mathbf{1}_l \rangle \\
 &= \hat{C}(T_n) + \mathbf{0} \oplus \langle \mathbf{1}_{l'} \rangle^\perp.
 \end{aligned}$$

$l' < 8$ となるので,

$$\text{Rad } \hat{C}(T_n) = (\hat{C}(T_n) * \hat{C}(T_n))^\perp \cap \text{Rad } \hat{C}(T_n) = \hat{C}(T_n)$$

となる. 従って, 補題 7 より, 極大性が言える. □

4 課題

ここまでで, 2 種類の極大 triply even code の構成法を述べたが, 現時点でその他の構成法は知られていない. 実際, 長さ 8, 16, 24, 32, 40, 48 について, 極大 triply even code の分類が与えられているが, いずれも前述の構成法 1 か構成法 2 によって得られる. (c.f. [1], [2])

存在, 非存在も含めた, これらの方法では構成できない極大な triply even code の解明が今後の課題である.

参考文献

- [1] K. Betsumiya, DATABASE: triply even codes of length 48, <http://www.st.hirosaki-u.ac.jp/~betsumi/triply-even/>.
- [2] K. Betsumiya and A. Munemasa, On triply even binary codes, J. London Math. Soc., **86** (1), 2012, 1–16.